(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号

特開平11－112491

(43)公開日　平成11年(1999)４月23日

(51)Int.Cl.[6]		識別記号	Ｆ Ｉ		
Ｈ０４Ｌ	9/14		Ｈ０４Ｌ	9/00	６４１
Ｇ０９Ｃ	1/00	６６０	Ｇ０９Ｃ	1/00	６６０Ｇ

審査請求　未請求　請求項の数４　ＯＬ　（全 8 頁）

(21)出願番号　特願平9－272793

(22)出願日　平成９年(1997)10月６日

(71)出願人　000003078
株式会社東芝
神奈川県川崎市幸区堀川町72番地

(72)発明者　加藤　岳久
東京都府中市東芝町１番地　株式会社東芝府中工場内

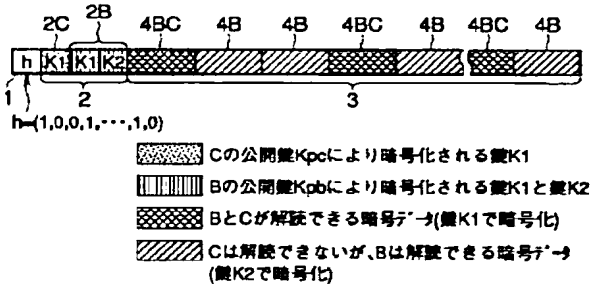
(74)代理人　弁理士　鈴江　武彦　（外６名）

(54)【発明の名称】　発信情報監視方法及び端末装置

(57)【要約】

【課題】　本発明は、例えば企業において暗号通信を行う場合に、外部へ秘密が漏洩することを防止しつつプライベート保護も実現する。

【解決手段】　データや通信文等の情報を暗号化して発信する際に用いられる発信情報監視方法において、情報３を複数のブロックに分割する分割ステップＳＴ４と、複数のブロックのうち一部のブロック４ＢＣを、発信情報を監視する者Ｃ及び受信者Ｂ双方に復号可能に暗号化する第１の暗号化ステップＳＴ４と、複数のブロックのうちの一部のブロックを除く他のブロック４Ｂを、受信者のみに復号可能に暗号化する第２の暗号化ステップＳＴ４とを有する発信情報監視方法。



1

【特許請求の範囲】
【請求項１】　送信データを含む伝送フレームを作成するフレーム作成部と、
前記フレームを複数のブロックに分割するフレーム分割処理部と、
前記複数のブロックのうちいくつかのブロックを第１の変換コードに基づいてコード化し、更に残りのブロックを第２の変換コードに基づいてコード化する変換処理部とを有することを特徴とする端末装置。
【請求項２】　データや通信文等の情報を暗号化して発信する際に用いられる発信情報監視方法において、
前記情報を複数のブロックに分割する分割ステップと、
前記複数のブロックのうち一部のブロックを、発信情報を監視する者及び受信者双方に復号可能に暗号化する第１の暗号化ステップと、
前記複数のブロックのうちの前記一部のブロックを除く他のブロックを、前記受信者のみに復号可能に暗号化する第２の暗号化ステップとを有することを特徴とした発信情報監視方法。
【請求項３】　前記複数のブロックのうち、何れのブロックが第１の暗号化ステップで暗号化されるかを示す識別情報を発信情報に付加するステップを有することを特徴とした請求項２記載の発信情報監視方法。
【請求項４】　前記第１の暗号化ステップ及び前記第２の暗号化ステップにおいては、前記複数のブロックのうち、それぞれどのブロックを暗号化するかを情報発信者に知られることなく、当該暗号化を行うことを特徴とした請求項２又は３記載の発信情報監視方法。
【発明の詳細な説明】
【０００１】
【発明の属する技術分野】この発明は発信情報監視方法及び端末装置、特にネットワークを用いてデータや通信文を暗号化して通信し合う場合に、その発信情報の監視に適した発信情報監視方法及び端末装置に関するものである。
【０００２】
【従来の技術】近年のネットワーク技術の発達、ネットワーク通信の活発化に伴い、公衆回線等の通信網上を流れる情報を悪意者等からいかに守るかということが極めて重要になってきている。
【０００３】このため、通信を行う際にそのデータや通信文を暗号化することが行われている。例えば社内ＬＡＮから公衆回線を通じて社外にデータや電子メール等を発信する場合、受信者のみがその情報を復号できるように発信者が発信情報に暗号化をかけるシステムの導入も検討されている。
【０００４】
【発明が解決しようとする課題】しかしながら、ネットワークを用いてデータや通信文を暗号化して通信を行う場合、その暗号化された情報が、例えば企業秘密のような企業外へ漏洩してはいけない情報か否かを監査することは従来の技術では困難である。

2

【０００５】一方、仮に社内ＬＡＮから発信されるすべての情報についてその内容を検査するシステムを構築したのでは、企業秘密情報のみならず、個人的な電子メール等の情報まですべて検査されることになる。しかし、これはプライベート保護の観点から妥当ではなく、また過度な情報監視は企業活動を停滞させてしまう可能性もある。
【０００６】本発明は、このような実情を考慮してなされたもので、例えば企業において暗号通信を行う場合に、外部へ秘密が漏洩することを防止しつつプライベート保護も実現する発信情報監視方法及び端末装置を提供することを目的とする。
【０００７】
【課題を解決するための手段】上記課題を解決するために、請求項１に対応する発明は、送信データを含む伝送フレームを作成するフレーム作成部と、フレームを複数のブロックに分割するフレーム分割処理部と、複数のブロックのうちいくつかのブロックを第１の変換コードに基づいてコード化し、更に残りのブロックを第２の変換コードに基づいてコード化する変換処理部とを有する端末装置である。
【０００８】本発明は、このような手段を設けたので、送信データを含む伝送フレームが複数のブロックに分割される。そして、この複数のブロックのうちいくつかのブロックが第１の変換コードに基づいてコード化され、更に残りのブロックが第２の変換コードに基づいてコード化される。このとき例えば、第１、第２の変換コードによりブロックを暗号化することも可能である。
【０００９】また、請求項２に対応する発明は、データや通信文等の情報を暗号化して発信する際に用いられる発信情報監視方法において、情報を複数のブロックに分割する分割ステップと、複数のブロックのうち一部のブロックを、発信情報を監視する者及び受信者双方に復号可能に暗号化する第１の暗号化ステップと、複数のブロックのうちの一部のブロックを除く他のブロックを、受信者のみに復号可能に暗号化する第２の暗号化ステップとを有する発信情報監視方法である。
【００１０】本発明は、このような手段を設けたので、例えば企業において暗号通信を行う場合に、外部へ秘密が漏洩することを防止しつつプライベート保護も実現させることができる。つまり発信情報をブロック化し、このブロックを受信者のみに解読できるブロックと、受信者及び監視者双方に解読できるブロックとにわけることで、秘密漏洩の有無を確認しつつ全発信情報を見ないことでプライベート保護をも図るものである。これは全発信情報を確認しなくても秘密漏洩の有無程度はチェックできることに着目したものである。
【００１１】さらに、請求項３に対応する発明は、請求

項２に対応する発明において、複数のブロックのうち、何れのブロックが第１の暗号化ステップで暗号化されるかを示す識別情報を発信情報に付加するステップを有する発信情報監視方法である。

【００１２】本発明は、このような手段を設けたので、請求項２に係る発明と同様な作用効果が得られる他、受信者は、この発信情報に付加された識別情報により、効率的に上記一部のブロックを監査し、また受信者は効率的に全ブロックを解読することができる。

【００１３】さらにまた、請求項４に対応する発明は、請求項２又は３に対応する発明において、第１の暗号化ステップ及び第２の暗号化ステップにおいては、複数のブロックのうち、それぞれどのブロックを暗号化するかを情報発信者に知られることなく、当該暗号化を行う発信情報監視方法である。

【００１４】本発明は、このような手段を設けたので、請求項２又は３に係る発明と同様な作用効果が得られる他、第１及び第２の暗号化ステップにおいては、複数のブロックのうち、それぞれどのブロックが暗号化されるかが情報発信者に対して秘密にされる。したがって、発信者は上記一部のブロックを特定できず、秘密情報を上記他のブロックに該当する部分に秘匿することができないため、秘密情報の発信監査をより一層効果的に行うことができる。

【００１５】

【発明の実施の形態】以下、本発明の実施の形態について説明する。

（発明の第１の実施の形態）図１は本発明の第１の実施の形態に係る発信情報監視方法が適用される場面を想定した図である。

【００１６】同図において、Ａは送信者でＢは受信者である。ＣはＡが発信する通信内容を監視する監査人である。このような場面は、例えばＡはある会社の社員であり、ＣはＡの会社の社長とする。ＢはＡとＣの会社以外の人間であると仮定する。

【００１７】本実施形態では、ＡとＢはＲＳＡ暗号方式等の公開鍵暗号を用いて暗号通信を行うものとする。ここでは、同図に示すように、Ａは公開鍵Ｋｐａと秘密鍵Ｋｓａを有しており、同様にＢは公開鍵Ｋｐｂと秘密鍵Ｋｓｂ、Ｃは公開鍵Ｋｐｃと秘密鍵Ｋｓｃを有している。なお、ＲＳＡ暗号（公開鍵暗号）を用いた暗号通信の方法については、「現代暗号理論」池野信一、小山謙二　共著、電子情報通信学会編、ｐ．１０５－１２３や「暗号理論入門」岡本栄司　著、共立出版株式会社、ｐ．８８－９９等にも記載されている。

【００１８】このような場合に、ＡがＢに向けて発信した個人的な秘密情報を全て第三者である監査人Ｃに知られることなく、ＡがＢに向けて発信した内容が会社の秘密情報ではないかについて、すなわちＡが会社の秘密情報を漏洩していないかについて監査人Ｃが調べる方法を

説明する。

【００１９】図２は本実施形態の発信情報監視方法に適用される送信情報のデータ並びの一例を示す図である。同図に示すＡが送信するデータ並び、つまり送信パケット（例えばメール）においては、データ本体３の先頭に、ヘッダ情報部１と鍵情報部２とが順次付加されている。

【００２０】このデータ本体３は、等しい大きさのブロック４Ｂ，４ＢＣ（以下、単にブロック４ともいう）に分割されている。このブロック４の大きさは、例えば暗号化を行うためのブロックの大きさである。

【００２１】このブロック４のうち、一部（全部を含む）のブロック４ＢＣのみ監査人Ｃにより復号できるようになっている。監査人Ｃは自己の復号可能なブロック４ＢＣを決定し、このヘッダ情報はＡには知らせない。

【００２２】図２においてヘッダ情報部１には、どのブロックが監査人Ｃが復号できるのかがヘッダ情報ｈとして格納されている。なお、同図に例示されるヘッダ情報ｈにおいて、ｈ＝１の部分は暗号ブロック４ＢＣに対応し、ｈ＝０の部分が暗号ブロック４Ｂに対応している。

【００２３】このように、監査人Ｃが復号できるブロック４ＢＣがＡにより特定できないようにすることで、発信者Ａは、漏洩してはいけない秘密情報を監査人Ｃに発見できないように操作することが不可能となる。

【００２４】図２の例では、ブロック４ＢＣが監査人Ｃと受信者Ｂが復号できる，すなわち鍵Ｋ１で暗号化された暗号ブロックであり、ブロック４Ｂが受信者Ｂのみが復号できる，すなわち鍵Ｋ２で暗号化された暗号ブロックである。

【００２５】各ブロック４について、ブロック４ＢＣはＢ，Ｃが復号でき、ブロック４ＢはＢのみが復号できるのは、ブロック４ＢＣを暗復号化する鍵Ｋ１と、ブロックＢを暗復号化する鍵Ｋ２とが暗号化されて鍵情報部２に格納されているからである。

【００２６】鍵情報部２は、Ｂ用鍵部２ＢとＣ用鍵２Ｃからなっている。Ｂ用鍵部２Ｂは、Ｂの公開鍵Ｋｐｂにより暗号化された鍵Ｋ１及び鍵Ｋ２が格納されており、Ｂの秘密鍵Ｋｓｂのみにより鍵Ｋ１及び鍵Ｋ２の取出しが可能である。一方、Ｃ用鍵部２Ｃは、Ｃの公開鍵Ｋｐｃにより暗号化された鍵Ｋ１のみが格納されており、Ｃの秘密鍵Ｋｓｃのみにより鍵Ｋ１の取出しが可能である。

【００２７】したがって、この送信パケットから監査人Ｃは、鍵Ｋ１のみを得ることができ、ブロック４ＢＣのみを監査することができる。一方、受信者Ｂは、この送信パケットから鍵Ｋ１及びＫ２を得ることができ、ブロック４ＢＣ及びブロック４Ｂ、すなわちデータ本体３のすべてを読むことができる。

【００２８】次に、この発信情報監視方法を実現するシステムの一例について具体的に説明する。図３は本実施

形態に係る発信情報監視方法を適用するネットワークシステムの構成例を示すブロック図である。

【００２９】このネットワークシステムは、通信手段としての公衆回線網１１を介してＣ社ＬＡＮ１２とＢ用システム１３が接続されて構成されている。Ｃ社ＬＡＮ１２においては、データ伝送路２１に、社員Ａの使用するＡ用端末２２の他、Ａ用端末２２と同様な構成の他の社員用の端末２３が複数接続され、さらに、Ｃ用端末２４、メールサーバ２５及びその他図示しないホスト計算機等が接続されている。

【００３０】メールサーバ２５は、ネットワーク接続装置を兼ねるものであり、公衆回線網１１を介してメールを授受すると共に、Ｃ社ＬＡＮ１２のデータ伝送路２１上のメールを取り込み、所定の規則に従って公衆回線網１１に送出するようになっている。

【００３１】Ａ用端末２２や端末２３は、文書やデータ作成等の基本的な計算機機能を実行できる他、メーラ２６が設けられ、作成したデータや文書をメールサーバ２５を介して公衆回線網１１に送出できるようになっている。

【００３２】メーラ２６は、ヘッダ付加部２７及び暗号化部２８を備え、暗号化された上記送信パケットにあて先等の必要な情報を付加し、メールとしてデータ伝送路２１上に送出する。

【００３３】ヘッダ付加部２７は、メール送信の際に、Ｃ用端末２４からヘッダ情報ｈを受け取るとともに、そのヘッダ情報ｈを暗号化部２８に通知し、暗号化部２８により暗号化されたデータ本体３及び鍵情報部２に、ヘッダ情報部１を付加する。なお、ヘッダ付加部２７は、発信者Ａの操作によってはヘッダ情報ｈを読み出すことができないように構成されており、メール発信前に発信者Ａがヘッダ情報ｈの内容を知ることはない。

【００３４】暗号化部２８は、ヘッダ付加部２７から受けたヘッダ情報ｈに基づき、データ本体３をブロックに分割し暗号化すると共に、そのデータ本体３を暗号化するのに用いた鍵をさらに暗号化して鍵情報部２に格納する。

【００３５】一方、Ｃ用端末２４は、監視ブロック設定部２９を備えＣ社ＬＡＮ１２から発信されるデータ（メール）の監査するブロックを設定可能になっている他、メールサーバ２５に対してＣ社ＬＡＮ１２から発信されるすべてのメールについて監査できるようになっている。さらに、メールサーバ２５がどのような条件でメールを発信するかを設定できるようになっている。

【００３６】監視ブロック設定部２９は、Ｃが監査できるブロック４ＢＣを決定する情報であるヘッダ情報を生成する。監視ブロック設定部２９の機能である監査人Ｃが復号できるブロック数ｎの決定方法としては、例えばＡが送信する情報の総ブロック数ｍを上限とし、ランダムな正の整数０＜ｎ＜ｍを生成する方法がある。また、

この下限と上限は監査人Ｃが任意に決定するようにしてもよい。

【００３７】また、監視ブロック設定部２９が監査人Ｃが復号できるブロック４ＢＣをどのような配置とするかは、例えばＡがＢに対して通信を行う日付や時間情報を元に、ランダム変数を決定することで行う。

【００３８】なお、このヘッダ情報ｈは秘密情報であり、監査人Ｃ以外は知ることができないよう各部２９，２６，２７，２８等は構成されている。また、上記したメールサーバ２５に設定する条件というのは、例えば監査済みのメールのみを発信可能とするとか、また例えばメールサーバ２５が取り込んでから所定時間を経過したメールのみを発信するようにするとか、さらに監査人Ｃが指定した所定の発信人のメールのみを監査終了まで発信しないようにする等が考えられる。

【００３９】次に、以上のように構成された本発明の実施の形態に係る発信情報監視方法を適用したシステムの動作について説明する。図４は本実施形態の発信情報監視方法を適用したシステムの動作を示す流れ図である。

【００４０】まず、監査人によって、ヘッダ情報の設定がなされる（ＳＴ１）。この情報設定は、Ｃ社ＬＡＮ１２に接続された端末２２，２３すべてについて一括で行ってもよく、また、個々に行ってもよい。ここでは監視ブロック設定部２９により、予めヘッダ情報が決定されている。

【００４１】次に、発信者Ａにより送信されるデータが作成され、さらに暗号化通信に必要なＢの公開鍵Ｋｐｂ及びＣの公開鍵Ｋｐｃが用意される（ＳＴ２）。なお、公開鍵Ｋｐｂ，Ｋｐｃは、暗号化部２８に事前に登録されている。

【００４２】次に、発信者Ａによりメーラ２６に対してデータの送信依頼が行われる（ＳＴ３）。これにより、メーラ２６により監視ブロック設定部２９からヘッダ情報が要求され、取得されたヘッダ情報に基づき、発信データのブロック化が行われる。さらに、監査人Ｃの復号できるブロック４ＢＣが鍵Ｋ１、監査人Ｃが復号できず受信者Ｂのみが復号できるブロック４Ｂが鍵Ｋ２により暗号化される（ＳＴ４）。なお、本動作例ではステップＳＴ１でヘッダ情報は予め決定されているとしたが、ヘッダ情報決定方法としては、上述したように例えば発信者Ａが受信者Ｂに対して通信を行う日付や時間情報を元に、ランダムにかつ個々にヘッダ情報を決定してもよい。このような決定方法を用いる場合には、上記ステップＳＴ１は、本ステップＳＴ４にてメーラ２６がヘッダ情報を監視ブロック設定部２９に要求したときに行われる。

【００４３】次に、鍵Ｋ１が監査人Ｃの公開鍵Ｋｐｃで暗号化され、また鍵Ｋ１及び鍵Ｋ２が受信者Ｂの公開鍵Ｋｐｂで暗号化され（ＳＴ５）、暗号化されたデータ本体３に鍵情報部２、ヘッダ情報１が付加され、メール用

の送信パケットが完成される。

【００４４】こうして完成されたパケットがメーラ２６によりデータ伝送路２１に送出され、メールサーバ２５により、このパケットが取得される（ＳＴ７）。このメールサーバ２５に格納されたパケット（Ｂ宛メール）は監査人Ｃにより監査される。すなわち監査人Ｃは、自分の公開鍵Ｋｐｃで暗号化された鍵Ｋ１を自分の秘密鍵Ｋｓｃで復号して、鍵Ｋ１を取り出す。なお鍵Ｋ２は取り出すことができない。監査人Ｃは、ヘッダ情報ｈに基づき、取り出した鍵Ｋ１により解読可能なブロック４ＢＣのみを復号し内容を確認する（ＳＴ８）。

【００４５】監査後、メールサーバ２５によりＢ宛のメール（送信パケット）が公衆回線上に送出され、Ｂ用システム１３で受信される（ＳＴ９）。メールを受け取った受信者Ｂは自分の秘密鍵Ｋｓｂを用いて、自分の公開鍵Ｋｐｂで暗号化された鍵Ｋ１と鍵Ｋ２を復号し取り出す。そしてヘッダ情報ｈに基づいて、鍵Ｋ１で暗号化されたブロック４ＢＣを復号し、かつ鍵Ｋ２で暗号化されたブロック４Ｂを復号する。これによりメール内の全情報を解読することができる。

【００４６】上述したように、本発明の実施の形態に係る発信情報監視方法は、発信者Ａが発信するデータを複数のブロックに分割すると共に、各ブロックを監査人Ｃと受信者Ｂが復号可能に暗号化されたブロック４ＣＢと、受信者Ｂのみが復号可能に暗号化されたブロック４Ｂの何れかとして送信パケットを構成するようにしたので、発信情報が例えば企業秘密のような秘密情報でないかを監査人が監査することができる。これにより企業秘密等の秘密情報の漏洩を防止することができるとともに、発信者は通信内容を全て監査人に開示することなく相手（受信者）に暗号通信を行うことができる。なお、受信者は通信内容を全て復号できる。

【００４７】また、復号するための鍵を監査人のみが復号できる鍵と、相手（受信者）が復号できる鍵とに分けて送信することにより、第３者に通信を盗聴することを防止することができる。

（発明の第２の実施の形態）本実施形態は、第１の実施形態とは異なる形式の送信パケットを用いることで機密情報漏洩を監視する方法について説明する。

【００４８】図５は本発明の第２の実施の形態に係る発信情報監視方法が適用される場面を想定した図であり、図１と同一部分には同一符号を付してその説明を省略する。同図に示す場合、発信者Ａと受信者Ｂはお互いが共有する秘密鍵である共有鍵Ｋｓａｂを持っている。監査人Ｃはこの共有鍵Ｋｓａｂがどのようなものであるかを知らない。

【００４９】図６は本実施形態の発信情報監視方法に適用される送信情報のデータ並びの一例を示す図であり、図２と同一部分には同一符号を付してその説明を省略する。この送信パケットは、ヘッダ情報部１と鍵情報部２とデータ本体３とから構成されている。また、本実施形態ではＢ用鍵部２Ｂ′に共有鍵Ｋｓａｂで暗号化された鍵Ｋ１が格納され、Ｂのみが解読できるブロック４Ｂ′が共有鍵Ｋｓａｂで暗号化されている点を除けば第１の実施形態と同様に構成されている。なお、図６に例示するヘッダ情報ｈとブロック４ＢＣ，４Ｂ′の対応関係は第１の実施形態と同様である。

【００５０】また、この発信情報監視方法を適用したシステムも図３に示す第１の実施形態と同様に構成されている。ただし、暗号化に共有鍵Ｋｓａｂが用いられ、かつ、図６のパケットが作成されるように暗号化部２８の構成が変更される点が第１実施形態と異なっている。

【００５１】次に、本実施形態の発信情報監視方法における処理の流れについて説明する。システム全体の動作は図４に示す処理流れと同様である。パケット構成及び使用する鍵の相違による第１実施形態との処理の違いについて説明する。

【００５２】本実施形態では、図４のステップＳＴ４において監査人Ｃが復号できるブロック４ＢＣは鍵Ｋ１で暗号化される。また、ステップＳＴ５にて鍵Ｋ１は監査人Ｃの公開鍵Ｋｐｃで暗号化され、Ｃ用鍵部２Ｃに格納される。

【００５３】一方図４のステップＳＴ４において、監査人Ｃが復号できずＢのみが復号できるブロック４Ｂ′は、共有鍵Ｋｓａｂで暗号化される。また、ステップＳＴ５にて鍵Ｋ１が共有鍵Ｋｓａｂで暗号化され、Ｂ用鍵部２Ｂ′に格納される。なお、鍵Ｋ１は第１実施形態と同様にＢの公開鍵Ｋｐｂにて暗号化してもよい。

【００５４】またブロックが監査人Ｃが復号できるブロック４ＢＣ、すなわち鍵Ｋ１で暗号化したブロック４ＣＢか否かを示す情報ｈは、第１実施形態と同様にヘッダ情報部１に納められる。

【００５５】こうしてメーラ２６により作成されたパケットはメールサーバ２５に送出される。監査人Ｃはメールサーバ２５にアクセスし、自分の公開鍵Ｋｐｃで暗号化された鍵Ｋ１を自分の秘密鍵Ｋｓｃで復号して、鍵Ｋ１を取り出す。なお、共有鍵Ｋｓａｂは知らない。このため監査人Ｃは、ヘッダ情報ｈに基づいて、鍵Ｋ１で暗号化されたブロックのみ復号する。

【００５６】一方、送信パケットを受信した受信者Ｂは、送信者Ａとの共有鍵Ｋｓａｂを用いて、共有鍵Ｋｓａｂで暗号化された鍵Ｋ１を復号し取り出す。そしてヘッダ情報ｈに基づいて、鍵Ｋ１で暗号化されたブロックを復号し、かつ共有鍵Ｋｓａｂで暗号化されたブロックを復号する。

【００５７】上述したように、本発明の実施の形態に係る発信情報監視方法は、第１の実施形態と同様な手段を設けた他、ブロック４Ｂを共有鍵Ｋｓａｂで暗号化するようにしたので、第１の実施形態と同様な効果を得ることができる。また、本実施形態の場合には、受信者Ｂの

共有鍵Ｋｓａｂを用いることで、受信者Ｂが公開鍵方式の公開鍵及び秘密鍵を有する必要をなくすことができる。

【００５８】なお、本発明は、上記各実施の形態に限定されるものでなく、その要旨を逸脱しない範囲で種々に変形することが可能である。例えば第１の実施形態では、Ａ，Ｂ，Ｃが公開鍵及び秘密鍵を有する場合を説明し、第２の実施形態では、ＡとＢが共有鍵Ｋｓａｂを有する場合で説明したが、各人が所有する鍵及び対応する暗号化についてはこのような場合に限られるものではない。つまり、種々の暗号化方式や各人の種々な鍵所有ケースに適宜対応して本発明を適用できるものである。

【００５９】また例えば上記各実施形態では、ヘッダ情報ｈをまとめてパケットの先頭に付加するようにしたが、ヘッダ情報ｈの付加方法は、このような方法に限られるものではない。

【００６０】図７はヘッダ情報ｈ夫々を対応するブロックの先頭に別々に設けた場合における送信情報のデータ並びの一例を示す図である。このようにヘッダ情報ｈは、図２や図６に示すようにヘッダ情報部１としてまとめて設けてもよいし、図７に示すように各暗号ブロック４の前に分散されたヘッダ情報部１′として設けてもよい。

【００６１】また、実施形態に記載した手法は、計算機（コンピュータ）に実行させることができるプログラム（ソフトウエア手段）として、例えば磁気ディスク（フロッピーディスク、ハードディスク等）、光ディスク（ＣＤ－ＲＯＭ、ＤＶＤ等）、半導体メモリ等の記憶媒体に格納し、また通信媒体により伝送して頒布することもできる。なお、媒体側に格納されるプログラムには、計算機に実行させるソフトウエア手段（実行プログラムのみならずテーブルやデータ構造も含む）を計算機内に構成させる設定プログラムをも含むものである。本装置を実現する計算機は、記憶媒体に記録されたプログラムを読み込み、また場合により設定プログラムによりソフトウエア手段を構築し、このソフトウエア手段によって動作が制御されることにより上述した処理を実行する。

【００６２】

【発明の効果】以上詳記したように本発明によれば、発信者により暗号化された情報を監査人により部分的に復号できるようにしたので、例えば企業において暗号通信を行う場合に、外部へ秘密が漏洩することを防止しつつプライベート保護も実現する発信情報監視方法及び端末装置を提供することができる。

【図面の簡単な説明】

【図１】本発明の第１の実施の形態に係る発信情報監視方法が適用される場面を想定した図。

【図２】同実施形態の発信情報監視方法に適用される送信情報のデータ並びの一例を示す図。

【図３】同実施形態に係る発信情報監視方法を適用するネットワークシステムの構成例を示すブロック図。

【図４】同実施形態の発信情報監視方法を適用したシステムの動作を示す流れ図。

【図５】本発明の第２の実施の形態に係る発信情報監視方法が適用される場面を想定した図。

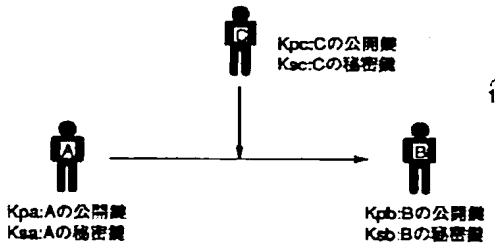
【図６】同実施形態の発信情報監視方法に適用される送信情報のデータ並びの一例を示す図。

【図７】ヘッダ情報ｈ夫々を対応するブロックの先頭に別々に設けた場合における送信情報のデータ並びの一例を示す図。

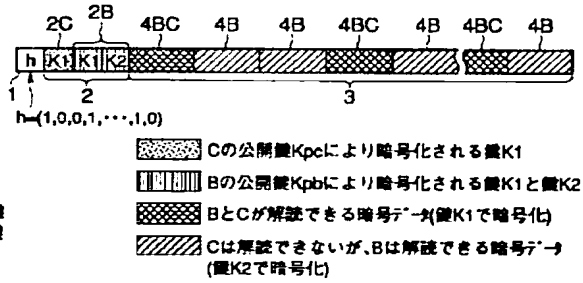
【符号の説明】

１…ヘッダ情報部
２…鍵情報部
２Ｂ…Ｂ用鍵部
２Ｃ…Ｃ用鍵部
３…データ本体
４Ｂ…Ｂのみが復号できるブロック
４ＢＣ…Ｂ及びＣが復号できるブロック
１１…公衆回線網
１２…Ｃ社ＬＡＮ
１３…Ｂ用システム
２１…データ伝送路
２２…Ａ用端末
２３…Ａ以外の社員が使用する端末
２４…Ｃ用端末
２５…メールサーバ
２６…メーラ
２７…ヘッダ付加部
２８…暗号化部
２９…監視ブロック設定部
Ａ…発信者
Ｂ…受信者
Ｃ…監査人
Ｋ１…鍵
Ｋ２…鍵
Ｋｐａ…Ａの公開鍵
Ｋｐｂ…Ｂの公開鍵
Ｋｐｃ…Ｃの公開鍵
Ｋｓａ…Ａの秘密鍵
Ｋｓａｂ…Ａ，Ｂの共有鍵
Ｋｓｂ…Ｂの秘密鍵
Ｋｓｃ…Ｃの秘密鍵
ｈ…ヘッダ情報

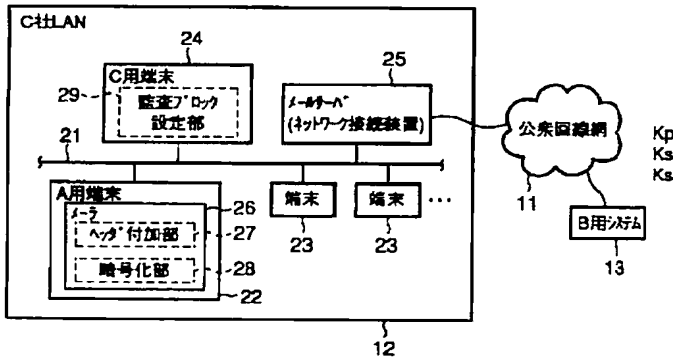
【図１】



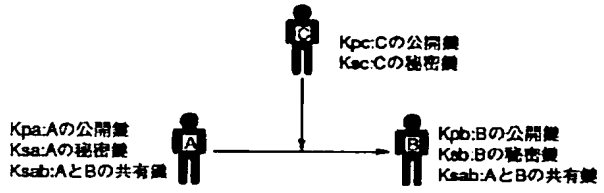
【図２】



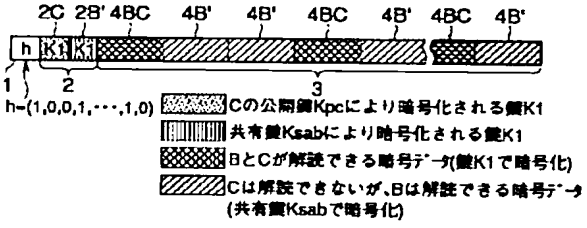
【図３】



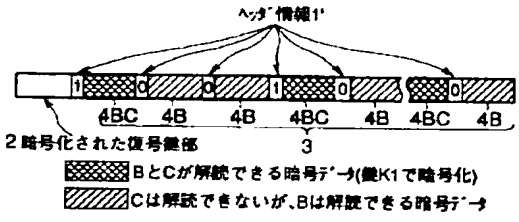
【図５】



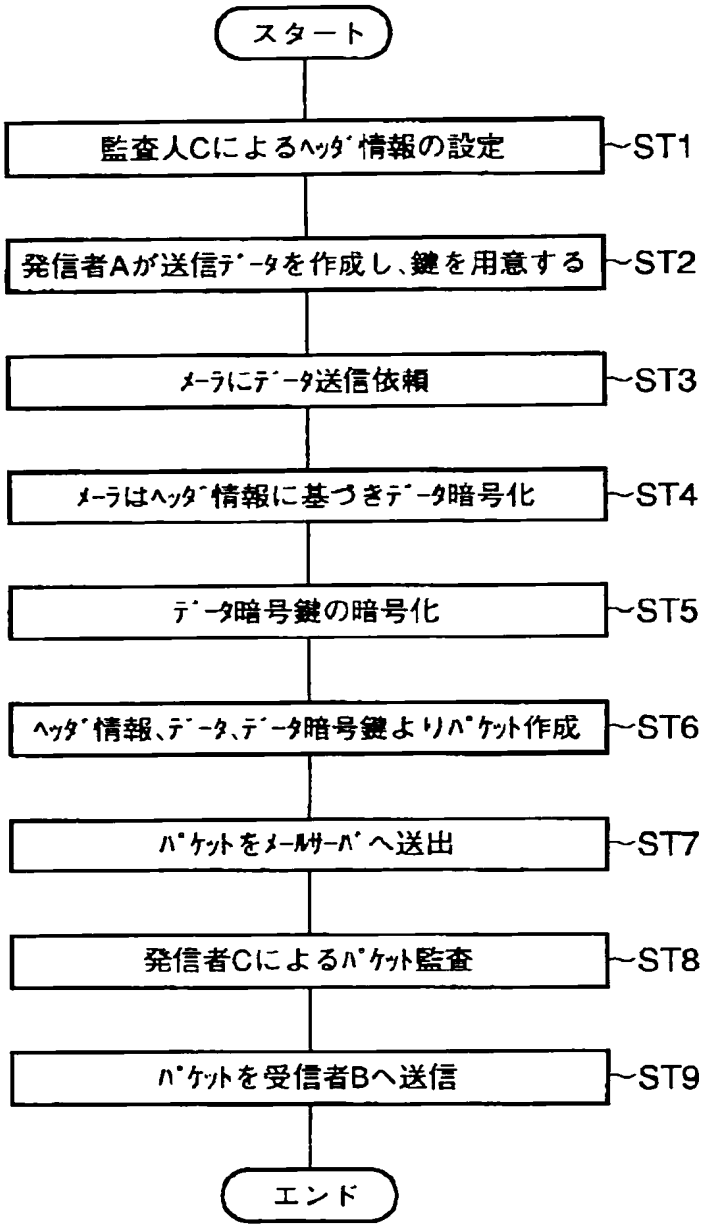
【図６】



【図７】



【図４】


スタート
監査人Cによるﾍｯﾀﾞ情報の設定
ST1
発信者Aが送信ﾃﾞｰﾀを作成し、鍵を用意する
ST2
ﾒｰﾗにﾃﾞｰﾀ送信依頼
ST3
ﾒｰﾗはﾍｯﾀﾞ情報に基づきﾃﾞｰﾀ暗号化
ST4
ﾃﾞｰﾀ暗号鍵の暗号化
ST5
ﾍｯﾀﾞ情報、ﾃﾞｰﾀ、ﾃﾞｰﾀ暗号鍵よりﾊﾟｹｯﾄ作成
ST6
ﾊﾟｹｯﾄをﾒｰﾙｻｰﾊﾞへ送出
ST7
発信者Cによるﾊﾟｹｯﾄ監査
ST8
ﾊﾟｹｯﾄを受信者Bへ送信
ST9
エンド